

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP04/053514

International filing date: 15 December 2004 (15.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: DE  
Number: 103 61 465.6  
Filing date: 23 December 2003 (23.12.2003)

Date of receipt at the International Bureau: 23 March 2005 (23.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

# BUNDESREPUBLIK DEUTSCHLAND

EP 04 / 53514



## Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

**Aktenzeichen:** 103 61 465.6

**Anmeldetag:** 23. Dezember 2003

**Anmelder/Inhaber:** Endress + Hauser GmbH+Co KG,  
79689 Maulburg/DE

**Bezeichnung:** Prozessmessgerät mit erweiterter  
Hardwarefehlererkennung

**IPC:** G 01 D 21/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 17. Januar 2005  
**Deutsches Patent- und Markenamt**  
Der Präsident  
Im Auftrag



Schiff

## **Prozessmessgerät mit erweiterter Hardwarefehlererkennung**

Die vorliegende Erfindung betrifft ein Prozessmessgerät, insbesondere ein  
5 Prozessmessgerät mit erweiterter Hardwarefehlererkennung.

Die Zertifizierung eines Prozessmessgerätes nach der Norm IEC61508;  
(SIL2) erfordert, dass am Gerät eventuell auftretende Hardware-Defekte mit  
hoher Wahrscheinlichkeit erkannt und als Fehlerzustand an einen  
10 Messwertempfänger signalisiert werden. Der statistische Anteil von Fehlern,  
die zu einer korrekten Signalisierung des Fehlerzustands an den  
Messwertempfänger führt, wird SFF (nach dem englischen Begriff Safe  
Failure Fraction) bezeichnet.

15 Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein  
Prozessmessgerät mit einer Im Sinne einer hohen  
Erkennungswahrscheinlichkeit im Falle von Hardwarefehlern bereitzustellen.

Statistische Analysen der Fehlerhäufigkeit haben ergeben, dass  
20 insbesondere Prozessoren und andere hochintegrierte Halbleiterbauteile,  
beispielsweise Speicher und ASICs, maßgeblich zur statistischen  
Gesamtausfallrate eines Prozessmessgerätes beitragen.

Die Aufgabe wird gelöst durch ein Prozessmessgerät mit einem ersten  
25 Prozessor, welcher in ersten Verarbeitungszyklen mit einem ersten  
Algorithmus eine Messwertverarbeitung durchführt; und einen zweiten  
Prozessor, welcher hauptsächlich für die Koordination und/oder  
Kommunikation zuständig ist,

30 wobei ferner der zweite Prozessor in Zeitabständen, die größer sind als der  
erste Verarbeitungszyklus einen Kontrolldatensatz aus dem ersten  
Prozessor ausliest, und anhand des Kontrolldatensatzes den ersten

Algorithmus ausführt und die korrekte Funktion des ersten Prozessors verifiziert.

Der erste Prozessor ist vorzugsweise ein spezialisierter digitaler  
5 Signalprozessor mit sehr schnellen Verarbeitungszyklen. Der zweite  
Prozessor ist beispielsweise ein Microcontroller, der erheblich langsamer  
arbeitet als der digitale Signalprozessor.

Der Kontrolldatensatz kann beispielsweise Rohmesswerte eines Sensors  
10 und Zustandsvariablen sowie die von dem ersten Prozessor daraus  
errechneten zugehörigen Ergebniswerte enthalten. Die Verifizierung erfolgt  
beispielsweise durch direkten Vergleich des aus dem ersten Prozessor  
ausgelesenen Ergebnis mit dem Ergebnis aus der Durchführung des ersten  
Algorithmus durch den zweiten Prozessor.

15 Der zweite Prozessor umfasst einen Programmspeicher. Zusätzlich kann  
der zweite Prozessor gemäß einer Weiterbildung der Erfindung seinen  
Programmspeicher mittels einer Prüfsumme oder einem CRC (nach  
englischen Begriff Cyclic Redundancy Check) regelmäßig verifizieren.

20 Der zweite Prozessor umfasst weiterhin einen Schreib/Lesespeicher, den  
der zweite Prozessor gemäß einer Weiterbildung der Erfindung mittels  
Testpattern regelmäßig auf statische Fehler überprüfen kann.

25 Der zweite Prozessor umfasst zudem ein Rechenwerk, einen  
Schreib/Lesespeicher, welchen der zweite Prozessor gemäß einer  
Weiterbildung der Erfindung mittels Prüfalgorithmen regelmäßig auf  
statische Fehler überprüfen kann.

30 In einer Weiterbildung der Erfindung kann der zweite Prozessor die Daten  
im Programmspeicher des ersten Prozessors mit einem lokal gespiegelten  
Speicherbereich vergleichen und verifizieren.

Nach einem Aspekt der Erfindung kann der zweite Prozessor bekannte Konstanten im Datenspeicher des ersten Prozessors durch Vergleich mit lokal gespiegelten Werten verifizieren.

5

Nach einem weiteren Aspekt der Erfindung kann, der zweite Prozessor Konfigurationsregister des ersten Prozessors durch Vergleich mit lokal gespiegelten Werten regelmäßig verifizieren.

- 10 In einer Ausgestaltung der Erfindung umfasst das Prozessmessgerät eine 4..20 mA Zweidraht-Schnittstelle. Optional kann eine Watchdog-Schaltung die Funktion des zweiten Prozessors und eines zugehörigen Taktgebers überprüfen und im Fehlerfall unabhängig von dem ersten Prozessor und dem zweiten Prozessor über den 4..20 mA Signalstrom einen Fehler  
15 signalisieren.

Die Erfindung wird nun an einem in den Figuren dargestellten Ausführungsbeispiel erläutert. Es zeigt:

- 20 Fig. 1: Ein Blockschaltbild der Geräteelektronik  
eines erfindungsgemäßen Druckaufnehmers; und

Fig. 2: Ein Blockschaltbild zur Selbstüberwachung.

25

- Die in Fig. 1. dargestellte modulare Geräteelektronik des erfindungsgemäßen Druckaufnehmers umfasst eine Sensorelektronik 1 und eine Hauptelektronik 2. Die Hauptelektronik 2, verarbeitet Sensorsignale, welche über eine serielle Schnittstelle von einer Sensorelektronik  
30 empfangen werden.

Die Sensorelektronik umfasst im einzelnen ein Sensor-ASIC 12, dessen wesentliche Aufgabe es ist, Druck- sowie Temperatursignale einer Druckmesszelle 11 bzw. eines Primärsensors entgegenzunehmen und ggf. ihre Signalpegel zu normieren. Dazu stehen – je nach Messprinzip des Primärsensors - eine Stromquelle für resistive Sensoren und eine kapazitive Schnittstelle für kapazitive Drucksensoren zur Verfügung, an die jeweils absolut/relativ oder Differenzdruckmesszellen angeschlossen werden können. Die Normierung erfolgt über einstellbare Verstärker, sogenannte „Programmable Gain Amplifieres“ (PGA), in den Ausführungen als Differenz und Absolutverstärker. Danach werden die normierten Werte analog/digital (A/D) gewandelt und über eine serielle Schnittstelle an die Hauptelektronik 2 weitergegeben. Sensorspezifische Daten wie Kompensationskoeffizienten u. ä. auf einem Sensor-EEPROM 13 abgelegt.

Das ASIC 12 ist in der Lage, Überläufe in den internen Verstärkern und A/D-Wandlern zu erkennen und diese ebenfalls über die serielle Schnittstelle in Form eines Fehlertelegramms an die Hauptelektronik 2 zu melden.

Die Hauptelektronik 2 umfasst im wesentlichen folgende Komponenten:

Einen Druckprozessor 21 (ASIC mit integriertem Digitalen Signal Prozessor (DSP)), der u. a. als serielles Interface zur Sensorelektronik 1 wirkt, deren Rohdaten empfängt, und daraus den Ausgangswert berechnet. Je nach Betriebsart kann der Ausgangswert entweder Druck, Füllstand oder Durchfluss repräsentieren. Das Rechenergebnis wird beispielsweise als pulsweitenmoduliertes Signal (PWM) bereitgestellt. Eine weitere Funktionalität des Prozessors 21 ist die Generierung des Taktsignals für die komplette Messumformerelektronik.

Die Hauptelektronik umfasst weiterhin einen Kommunikations-ASIC 22; dieser Baustein dient als Schnittstelle des Messumformers zur Außenwelt. In ihm integriert ist ein DC/DC-Wandler zur Stromversorgung des gesamten

Gerätes und ein Stromsteller, der aus dem PWM-Signal des Druckprozessors den entsprechenden Stromwert auf eine 4–20mA Stromschleife einprägt. Weiterhin sind in ihm ein HART-Modem für die Kommunikation auf Feldebene, eine hochgenaue Spannungsreferenz sowie  
5 ein Hardware-Watchdog integriert.

Weiterhin umfasst die Hauptelektronik einen Microcontroller 25, welcher für die Initialisierung des Messprozessors benötigt wird. Im Regelbetrieb wird über ihn  
10 die Vor-Ort-Bedienung mittels Taster bzw. Fernbedienung über HART realisiert. Zu diesem Zweck kann auch noch ein Display 23 vorgesehen sein.

Weitere Funktionen des Microcontrollers 25 können beispielsweise Fehlerverarbeitung, Umrechnung der Messdaten in vom Benutzer  
15 eingestellte Einheiten, Triggern eines Watchdogs im Kommunikations-ASIC, Protokollieren von Min/Max-Werten und der Messbereichsüberschreitung, Summenzähler für den Modus „Durchfluss“, und Nichtflüchtige Datenhaltung sein.

20 Beim Druckprozessor 21 handelt es sich um ein ASIC mit einem integrierten digitalen Signalprozessor. Seine Stärke liegt in der schnellen und äußerst energiesparenden Berechnung der Messwerte. Unter Vollast beträgt die Stromaufnahme des Druckprozessors ca. 600 µA.

25 Der Microcontroller 25 ist zwar prinzipiell auch in der Lage, diese Berechnungen durchzuführen, allerdings würde er bei gleicher Berechnungsgeschwindigkeit ein Vielfaches an Energie verbrauchen; zu viel für ein Gerät, das seine Versorgung aus einer 4–20mA Stromschleife bezieht. Eingesetzt wird der Microcontroller in den Bereichen, wo es nicht  
30 auf zeitkritische Berechnungen ankommt. Dadurch ist es möglich, den Baustein mit einem stark reduzierten Takt zu betreiben, um den Stromverbrauch auf ein verträgliches Maß zu senken.

Bei der Geräteinitialisierung ist folgende Besonderheit zu beachten. Da es mehrere verschiedene Sensorbaugruppen und Hauptelektronikvarianten gibt, wäre es ein zu großer Aufwand, für jede mögliche Kombination von Sensor und Elektronik eine passende Softwarelösung bereitzustellen. Dies wird  
5 dadurch umgangen, dass man die Software in zwei Teile aufteilt, nämlich in einen sensor- und einen applikationsspezifischen Teil.

Der sensorspezifische Teil ist auf der Sensorelektronik in einem Sensor-EEPROM 13 gespeichert. Erhält die Sensorik die ersten Taktsignale von der Hauptelektronik, so liest sie ihren Programmteil aus dem EEPROM aus und schickt ihn über die serielle Verbindung an die Hauptelektronik. Dort wird das Sensorprogramm vom Microcontroller 25 aus dem DSP 21 ausgelesen und mit dem applikationsspezifischen Programm verbunden, das er aus  
15 dem Programmspeicher der Hauptelektronik erhält. Die beiden Programmteile werden dann miteinander verbunden, d.h. die Offsets der Adressen im Speicher werden so verändert, dass verschiedene Variablen nicht die gleichen Speicherbereiche verwenden. Nach Abschluss dieses Vorgangs wird das nun komplettierte Programm zurück in den DSP  
20 geschrieben. Danach werden lediglich noch die Konfigurationsparameter der Messumformung in den Datenspeicher des DSP geladen, der Messumformer ist nun einsatzbereit und berechnet aus den daraufhin eintreffenden Rohdaten die Messwerte.

25 Die erfindungsgemäßen Druckaufnehmer erfüllen vorzugsweise die Anforderungen an Funktionale Sicherheit bis SIL 2 nach IEC 61508. Die Norm stellt quantitative Anforderungen hinsichtlich der Einhaltung von Mindestwerten für sicherheitstechnische Kenngrößen wie Safe Failure Fraction (SFF) an die Geräte. Zur Erfüllung der quantitativen Anforderungen  
30 (z.B. SFF > 90%) sind in der Regel zusätzliche Diagnosemaßnahmen und Überwachungsfunktionen im Gerät erforderlich. Über eine FMEDA (Failure Mode, Effects and Diagnostics Analysis) der Elektronik auf



Komponentenebene mit nachfolgender Optimierung wurde die Selbstüberwachung, deren Konzept im folgenden beschrieben ist, als Beitrag zur Erfüllung der SIL2 Norm identifiziert.

- 5 Die Selbstüberwachung besteht aus einem Softwarepaket, mit dem unter anderem CRCs (Cyclic Redundancy Check) und Prüfsummen von RAM und ROM des Microcontrollers sowie des EEPROM realisiert werden.

10 Die Selbstüberwachung umfasst weiterhin eine stichprobenartigen Kontrolle der Funktion des DSP durch eine Kontrollrechnung im Microcontroller. Dazu müssen, wie in Fig. 2 gezeigt, die Eingangswerte und Zustandsvariablen sowie der Ausgangswert aus dem DSP 21 ausgelesen werden. Aus den Eingangswerten und den Zustandsvariablen wird der Ausgangswert berechnet, den der DSP ausgeben müsste. Danach wird der gemessene mit  
15 dem berechneten Ausgangswert verglichen. Kommt es dabei zu Differenzen, so wird dies an übergeordnete Kontrollinstanzen in der Software des Messumformers gemeldet, die ihrerseits veranlassen, dass der Kommunikations-ASIC 22 ein Fehlersignal (HART) ausgibt. Anhand dieses Signals erkennt das Auswertegerät, an dem der Messumformer  
20 angeschlossen ist, den Gerätefehler und leitet die notwendigen Maßnahmen ein, wie eine Meldung zum Austausch des defekten Gerätes.

Der DSP 21 auf der Hauptelektronik führt sehr schnelle Berechnungen durch. Um nun diesen Baustein überwachen zu können, wird eine  
25 Baugruppe benötigt, die zumindest ebenso schnell die Berechnungen durchführen oder zumindest die Daten des DSP kann. Es wurde im vorliegenden Ausführungsbeispiel die Selbstüberwachung durch den Microcontrollers 25 gewählt. Diese Lösung beinhaltet die Kontrollrechnung seitens des Microcontrollers 25. Sie kommt ohne zusätzliche Hardware aus und sorgt dabei noch mit diversitärer Hardware für eine erweiterte Sicherheit.  
30 Die geringere Geschwindigkeit des Microcontrollers 25 verhindert es aber,

die Berechnungen des DSP in Echtzeit durchzuführen. Dies ist zu berücksichtigen.

Der Microcontroller 25 führt daher nur Stichproben durch. Der einzig  
5 zeitkritische Vorgang ist dabei das Einlesen der Zustandsvariablen  
(zwischengespeicherte Werte des letzten Meßzyklus) und der Druck- und  
Temperaturrohdaten der Sensorelektronik sowie des berechneten  
Ausgangswertes des DSP 21. Die nachfolgende Berechnung des  
Ausgangswertes im  $\mu C$  ist praktisch zeitunabhängig, sie kann beliebig oft  
10 durch andere Programmteile unterbrochen werden.

Die Selbstüberwachung besteht in der Hauptsache aus drei Programmteilen:  
Einer Hauptroutine, der Erfassung der Messwerte, und einer eigenständigen  
Berechnung mit anschließendem Vergleich. Die komplette  
15 Selbstüberwachung ist in Form von Zustandsmaschinen realisiert, wobei für  
die Erfassung und die Berechnung absichtlich zwei getrennte Prozesse  
eingesetzt werden. Dies ermöglicht eine unterschiedliche Priorisierung der  
beiden Vorgänge auf Interruptebene. Die Messwernerfassung bedarf einer  
hohen Priorität, um einen kompletten, gültigen Datensatz in der gegebenen  
20 Zeit einlesen zu können. Liefte dieser Prozess auf einer niedrigeren Ebene,  
würde die Selbstüberwachung nicht funktionieren, da es aufgrund von  
Unterbrechungen nie zu einem kompletten Datensatz käme. Im Gegensatz  
dazu braucht die Berechnung keine hohe Priorität, da sie keinem Zeitzwang  
unterliegt.

25 Im sensor- und applikationsspezifischen Programm gibt es jeweils Variablen,  
die den Wert der vorherigen Messung enthalten (Dämpfungswerte,  
Rauschfilter). Dabei ist zu beachten, dass sich diese Werte sehr schnell  
ändern, da ein kompletter Programmdurchlauf im DSP weniger als 10 ms  
30 dauert. Für die Kontrollrechnung sind die Zahlenwerte zum relevanten  
Zeitpunkt erforderlich, da sonst ein bitgenauer Vergleich nicht möglich ist.  
Dies wird durch schnelles Einlesen der betroffenen Variablen unter

Verwendung von „Inline-Code“ erreicht, also mit optimiertem Code auf Assembler-Ebene, der auf das Aufrufen von Registern und langwierige Stackoperationen verzichtet.

- 5 Jedes neue Datenpaket, das den DSP erreicht, löst einen Interrupt aus, der sich auch für die Synchronisation der Selbstüberwachung einsetzen lässt. In der Interrupt-Routine wird bei jedem Aufruf automatisch ein Zähler (Framecounter) inkrementiert. Als zusätzliche Funktionalität ist das Einlesen der Statusvariablen bei einem bestimmten Stand des Framecounters integriert.
- 10

- Die Messwerterfassung beinhaltet das Einlesen der Druck- und Temperaturwerte des Sensor-ASIC, die zwischengespeicherten Ergebnisse der vorangegangenen Berechnung sowie den berechneten Ausgangswert des DSP. Nach dem Einlesen der Werte ist zu überprüfen, ob die
- 15 eingelesenen Werte, tatsächlich den gleichen Messzeitpunkt repräsentieren.

- Anschließend wird das DSP-Programm vom Microcontroller 25 ausgeführt, um die Kontrollrechnung anhand der eingelesenen Daten durchzuführen.
- 20 Nach dem Ende der Kontrollrechnung findet ein Vergleich von Rechen- und Messwert statt. Stellt der Microcontroller eine zu große Differenz zwischen Rechen- und Messwert fest, wird das Kommunikations-ASIC angewiesen, einen Fehlerstrom auszugeben und bei Bedarf noch eine Fehlermeldung über HART auszugeben.

**Patentansprüche**

1. Prozessmessgerät mit einem ersten Prozessor 21, welcher in ersten  
Verarbeitungszyklen mit einem ersten Algorithmus eine  
Messwertverarbeitung durchführt; und einen zweiten Prozessor 25,  
welcher Koordinations und/oder Kommunikationsaufgaben wahrnimmt,  
wobei ferner der zweite Prozessor 25 in Zeitabständen, die größer sind  
als der erste Verarbeitungszyklus einen Kontrolldatensatz aus dem  
ersten Prozessor 21 ausliest, und anhand des Kontrolldatensatzes den  
ersten Algorithmus ausführt um die korrekte Funktion des ersten  
Prozessors zu verifizieren.
2. Prozessmessgerät nach Anspruch 1, wobei der Kontrolldatensatz  
Rohmesswerte eines Sensors und Zustandsvariablen sowie die von  
dem ersten Prozessor daraus errechneten zugehörigen Ergebniswerte  
enthält.
3. Prozessmessgerät nach Anspruch 1 oder 2, wobei die Verifizierung  
durch direkten Vergleich des aus dem ersten Prozessor 21  
ausgelesenen Ergebnis mit dem Ergebnis aus der Durchführung des  
ersten Algorithmus durch den zweiten Prozessor 25 erfolgt.
4. Prozessmessgerät nach einem der Ansprüche 1 bis 3, wobei der  
zweite Prozessor einen Programmspeicher umfasst und den  
Programmspeicher mittels einer Prüfsumme oder einem CRC  
regelmäßig verifiziert.
5. Prozessmessgerät nach einem der Ansprüche 1 bis 4, wobei der  
zweite Prozessor weiterhin einen Schreib/Lesespeicher, den der zweite  
Prozessor mittels Testpattern regelmäßig auf statische Fehler  
überprüfen kann.

6. Prozessmessgerät nach einem der Ansprüche 1 bis 5, wobei der zweite Prozessor einen Schreib/Lesespeicher, welchen der zweite Prozessor mittels Prüfalgorithmen regelmäßig auf statische Fehler überprüfen kann.
- 5
7. Prozessmessgerät nach einem der Ansprüche 1 bis 6, wobei der zweite Prozessor die Daten im Programmspeicher des ersten Prozessors mit einem lokal gespiegelten Speicherbereich vergleicht und verifiziert.
- 10
8. Prozessmessgerät nach einem der Ansprüche 1 bis 7, wobei der zweite Prozessor bekannte Konstanten im Datenspeicher des ersten Prozessors durch Vergleich mit lokal gespiegelten Werten verifiziert.
- 15
9. Prozessmessgerät nach einem der Ansprüche 1 bis 8, wobei der zweite Prozessor Konfigurationsregister des ersten Prozessors durch Vergleich mit lokal gespiegelten Werten regelmäßig verifiziert.
- 20
10. Prozessmessgerät nach einem der Ansprüche 1 bis 9, wobei das Prozessmessgerät eine 4..20 mA Zweidraht-Schnittstelle umfasst, und wobei eine Watchdog-Schaltung die Funktion des zweiten Prozessors und eines zugehörigen Taktgebers überprüft und im Fehlerfall unabhängig von dem ersten Prozessor 21 und dem zweiten Prozessor 25 über den 4..20 mA Signalstrom einen Fehler signalisiert.

### Zusammenfassung

Ein Prozessmessgerät mit einem ersten Prozessor 21, welcher in ersten  
Verarbeitungszyklen mit einem ersten Algorithmus eine  
5 Messwertverarbeitung durchführt; und einen zweiten Prozessor 25, welcher  
Koordinations und/oder Kommunikationsaufgaben wahrnimmt. Der zweite  
Prozessor 25 liest in Zeitabständen, die größer sind als der erste  
Verarbeitungszyklus einen Kontrolldatensatz aus dem ersten Prozessor 21,  
und führt anhand des Kontrolldatensatzes den ersten Algorithmus aus um  
10 die korrekte Funktion des ersten Prozessors zu verifizieren.

(Fig. 2)

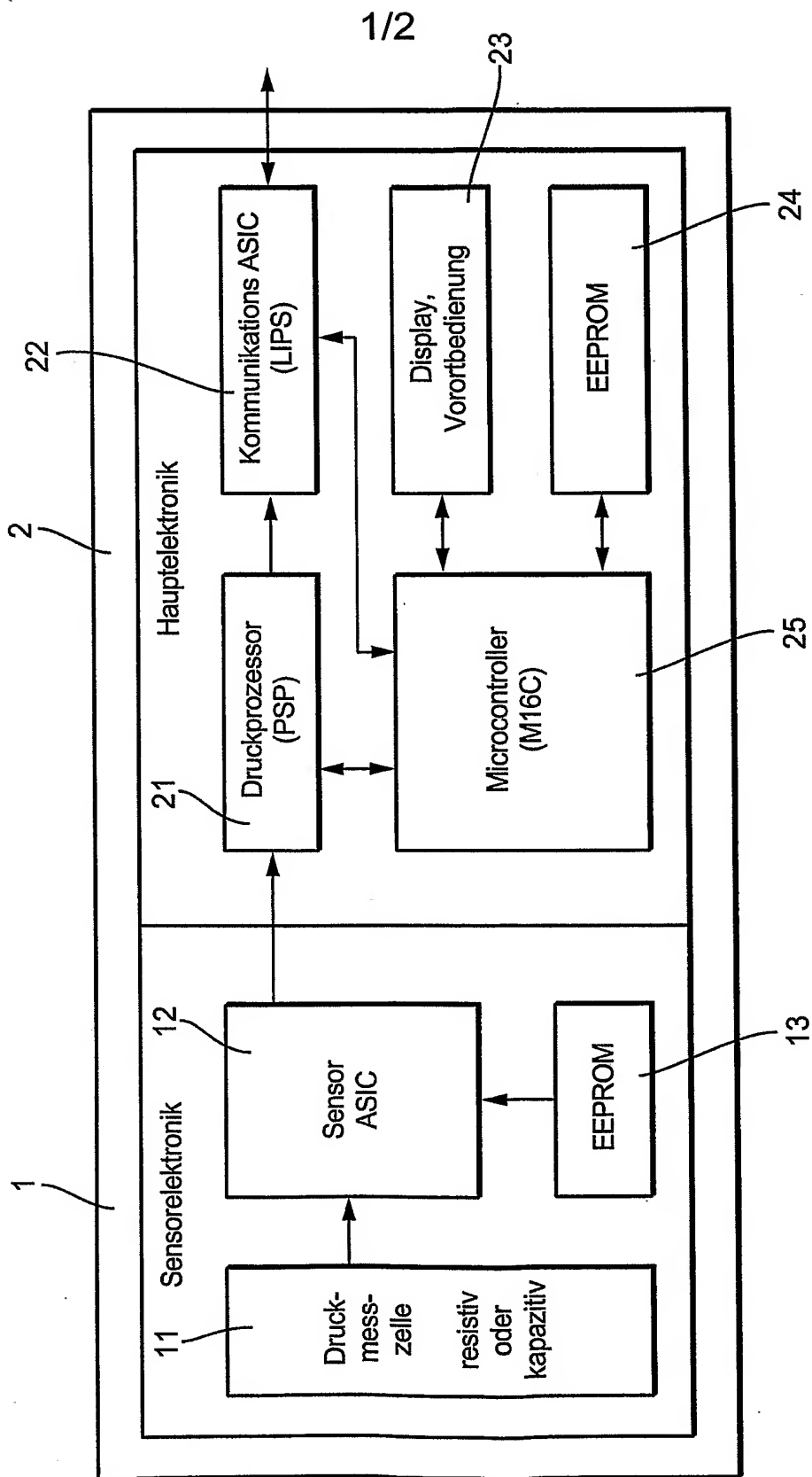


Fig. 1

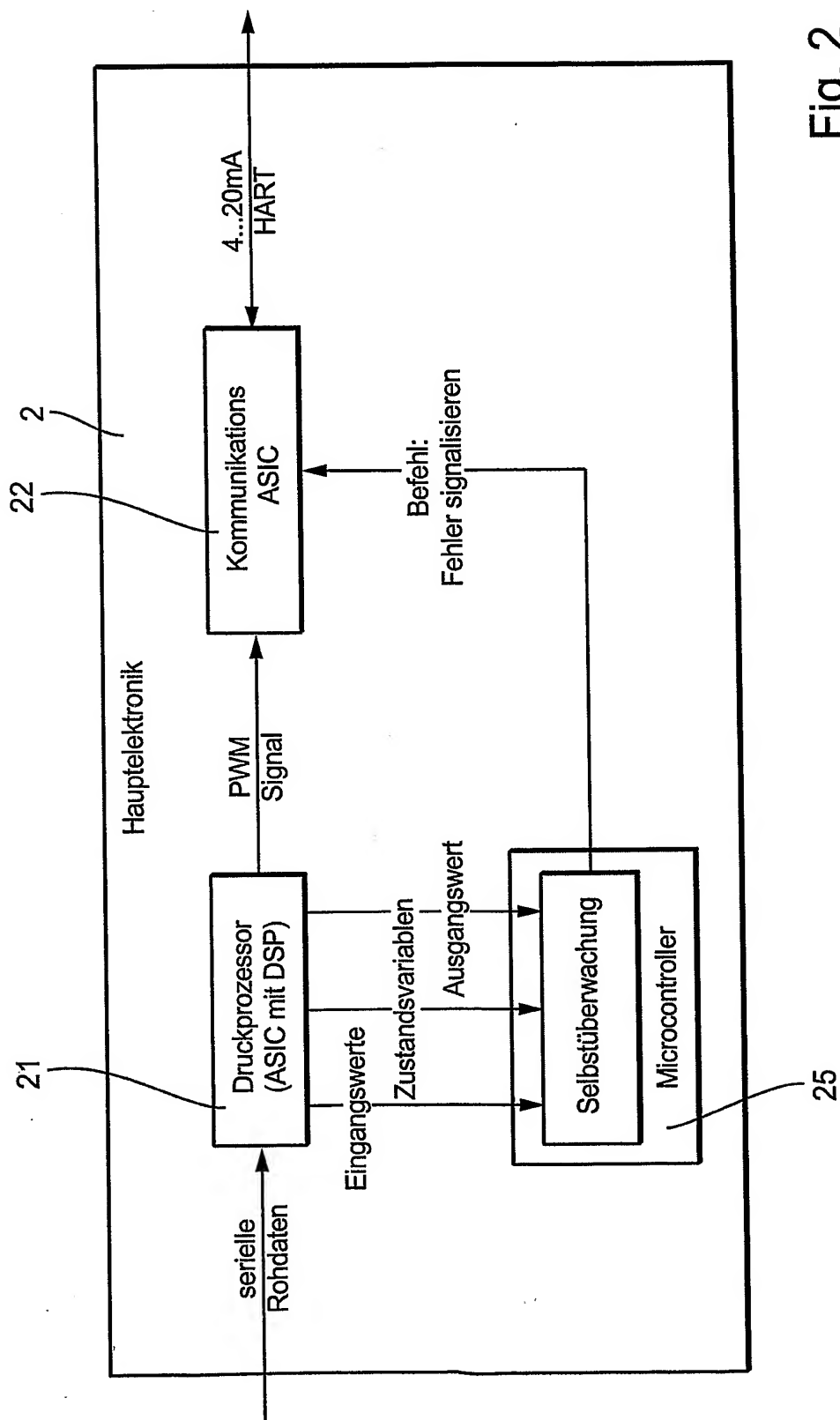


Fig. 2



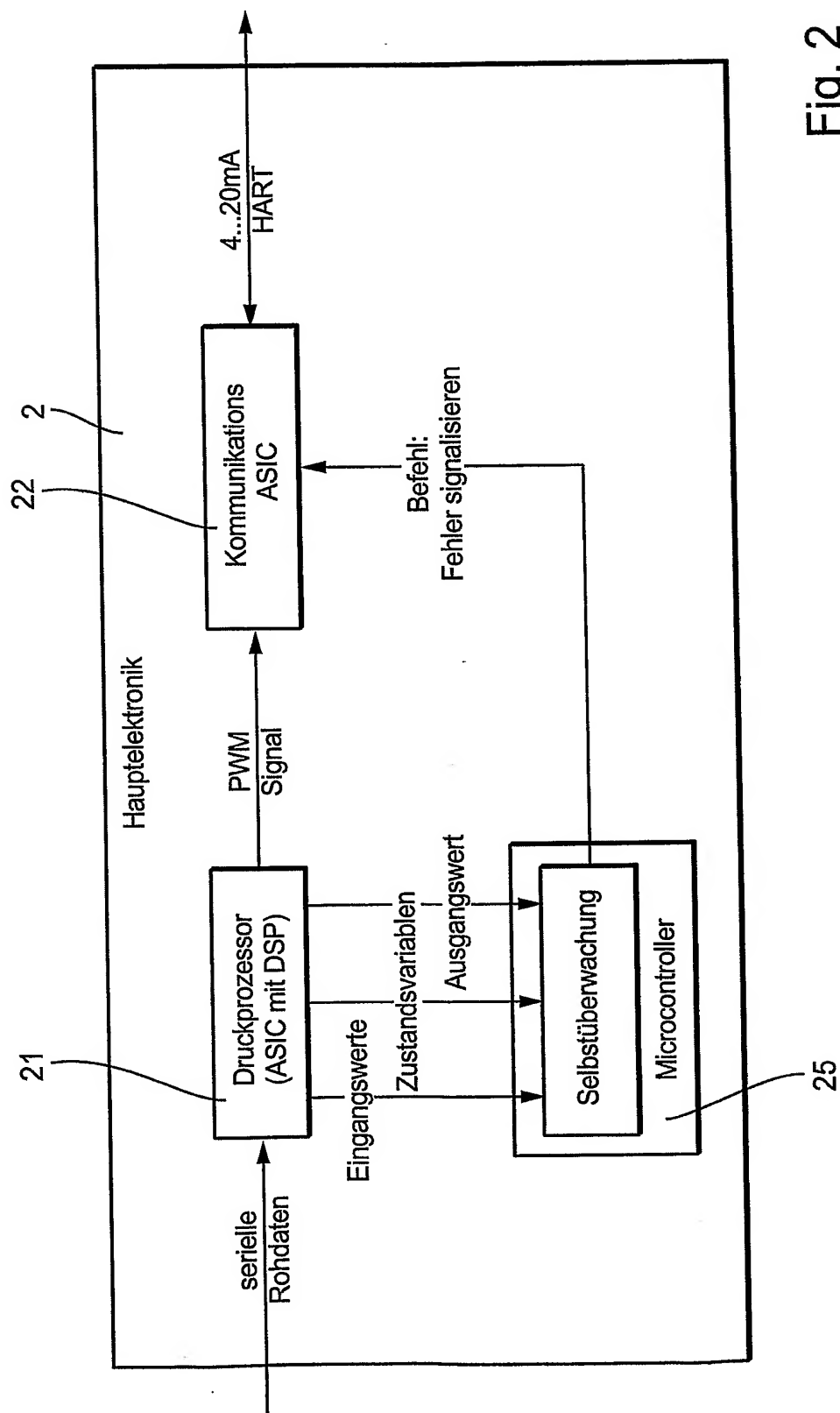


Fig. 2